Amendments to the Specification

Page 23, lines 7-14, please replace the existing paragraph with the following amended paragraph:

a1

The challenge input unit 9 is supplied with challenge c, which is query information for authentication. The response generation unit 10 generates response r from the challenge c inputted to the challenge input unit 9 and the hash value X(M) generated by the hash value calculation unit ~~6~~5. The response output unit 11 outputs the response r generated by the response generation unit 10.

Page 23, lines 18-27, please replace the existing paragraph with the following amended paragraph:

a2

It is assumed that the finite group G is difficult with discrete logarithm problems in the example of Diffie-Hellman key sharing, and is difficult with annihilators decision problems in the example of RSA. The hash value X(M) generated by the hash value calculation unit ~~6~~ 5 is an element of p element field F_p in the example of Diffie-Hellman key sharing, and an element of the finite ring Λ in the example of RSA. The challenge c inputted to the challenge input unit 9 is an element of the finite group G.

Page 24, lines 20-26, please replace the existing paragraph with the following amended paragraph:

a3

The random number generation unit 12 generates a random number k. The response generation unit 10 generates response r from the random number k generated by the random number generation unit 12, the challenge c inputted to the challenge input unit 9, and the hash value X(M) generated by the hash value calculation unit ~~6~~5.

Page 25, lines 10-18, please replace the existing paragraph with the following amended paragraph:

a4

The hash value X(M) generated by the hash value calculation unit ~~6~~ 5 and the random number k generated by the random number generation unit 12 are elements of the p-elements field F_p in examples of DSA signature, variants of ElGamal signature, Nyberg-Rueppel signature, and Schnorr signature, and are elements of the finite group G in examples of message recovery type Guillou-Quisquater signature, and Guillou-Quisquater signature.

Page 28, line 18 to page 29, line 1~~, please~~ replace the existing paragraph with the following amended paragraph:

a5

The random number generation unit 12 generates the random number k. The commitment generation unit 13 generates a commitment w from the random number k generated by the random number generation unit 12. The commitment output unit 14 outputs the commitment w generated by the commitment generation unit 13. The response generation unit 10 generates the response r from the random number k generated by the random number generation unit 12, the challenge c inputted to the challenge input unit 9, and the hash value X(M) generated by the hash value calculation unit ~~6~~5.

Page 29, lines 17-23, ~~please~~ replace the existing paragraph with the following amended paragraph:

a6

The hash value X(M) generated by the hash value calculation unit ~~6~~ 5 and the random number k generated by the random number generation unit 12 are elements of the p-elements field F_p in an example of Schnorr authentication, and are elements of the finite group G in examples of Guillou-Quisquater authentication and Fiat-Shamir authentication.

Page 32, lines 9-15, ~~please~~ replace the existing paragraph with the following amended paragraph:

a7

The response generation unit 10 generates the response r from the random number k generated by the random number generation unit 12, the commitment generated by the a7 cont

commitment w generation unit 13, the challenge c inputted to the challenge input unit 9, and the hash value X(M) generated by the hash value calculation unit ~~6~~5.

Page 32, lines 19-24, please replace the existing paragraph with the following amended paragraph:

a8

It is assumed that the finite group G is difficult with discrete logarithm problems. The hash value X(M) generated by the hash value calculation unit ~~6~~5, the random number k generated by the random number generation unit 12, and the challenge c inputted to the challenge input unit 9 are elements of the p element field F_p.

Page 59, lines 8-12, please replace the existing paragraph with the following amended paragraph:

a9

The right recipient (user) 35 holds the proving instrument (the second or fifth embodiment) ~~36~~ T having the private hash function H issued in association with the unique value d by the proving instrument issuing device (the sixth embodiment).